

## SIGNAL RECORDER

Publication number: JP2041091

Publication date: 1990-02-09

Inventor: HIRASHIMA MASAYOSHI; SATO TOSHICHIKA

Applicant: MATSUSHITA ELECTRIC IND CO LTD

Classification:

- international: **H04N5/92; H04N7/167; H04N7/169; H04N5/92; H04N7/167; H04N7/169; (IPC1-7): H04N7/167**

- European:

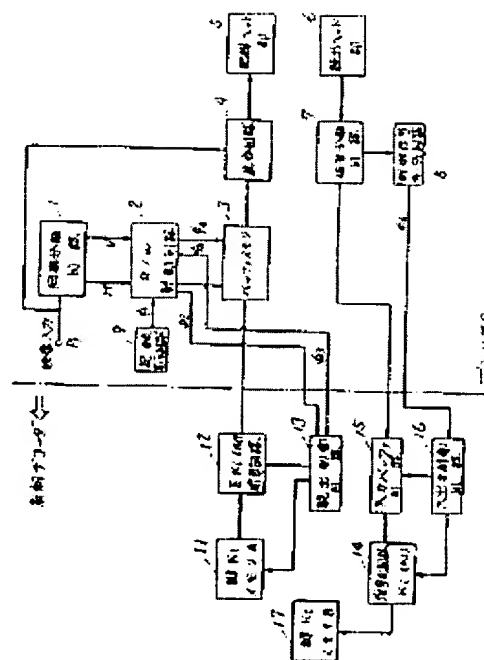
Application number: JP19880191782 19880729

Priority number(s): JP19880191782 19880729

Report a data error here

### Abstract of JP2041091

**PURPOSE:** To disable interception even if a reproducing signal is illegally copied by using a specific key at a charged decoder so as to encipher a decoding key and multiplexing it during the horizontal or vertical blanking period. **CONSTITUTION:** A key Kt in a Kt memory A11 is enciphered by using a specific key Ki at an enciphering device 12 to generate an enciphering key EKi (Kt) and it is stored in a buffer memory 3. The content of the memory 3 is read for a prescribed period and it is superimposed onto the nH-th TV signal. A mixing circuit 4 eliminates the nH-th scrambled video signal, the EKi (Kt) signal is superimposed and it is recorded on a tape by a recording head section 5. At reproduction, a readout head section 6 reads a recording signal, a decoding circuit 14 uses a key Ki specific to the charged decoder so as to decode the signal, the key Kt is extracted and written in a Kt memory B17. Thus, other charged decoder cannot descramble the signal, then illegal copy is prevented.



Data supplied from the **esp@cenet** database - Worldwide

⑤ Int. Cl.<sup>5</sup>

識別記号

庁内整理番号

④ 公開 平成2年(1990)2月9日

H 04 N 7/167

8725-5C

審査請求 未請求 請求項の数 1 (全6頁)

⑬ 発明の名称 信号記録装置

⑰ 特 願 昭63-191782

⑱ 出 願 昭63(1988)7月29日

⑲ 発 明 者 平 嶋 正 芳 大阪府門真市大字門真1006番地 松下電器産業株式会社内  
 ⑲ 発 明 者 佐 藤 寿 親 大阪府門真市大字門真1006番地 松下電器産業株式会社内  
 ⑲ 出 願 人 松下電器産業株式会社 大阪府門真市大字門真1006番地  
 ⑲ 代 理 人 弁理士 栗 野 重 孝 外1名

## 明 細 書

## 1、発明の名称

信号記録装置

## 2、特許請求の範囲

少なくともテレビジョン信号の映像信号と音声信号を記録再生する装置であって、スクランブル化されたテレビジョン信号を復号するデコーダからそのデコーダに固有の鍵 K<sub>1</sub> を用いて暗号化された解読鍵 K<sub>2</sub> を読み出すための駆動信号を出力する手段と、前記暗号化された解読鍵 K<sub>2</sub> をテレビジョン信号中の水平または垂直の帰線期間またはその近傍で記録可能な部分に多重化する手段と、再生信号から前記暗号化された解読鍵 K<sub>2</sub> を抽出し制御信号と共に前記デコーダへ前記再生信号を供給する手段とを備えたことを特徴とする信号記録装置。

## 3、発明の詳細な説明

産業上の利用分野

本発明は、有料テレビジョン放送のスクランブル化された映像信号を記録する信号記録装置に関

し、特にスクランブル化された信号を再生するための鍵の信号をデコーダから読み出し記録できるようにした信号記録装置に関する。

従来の技術

VTR等の録画装置の普及によりテレビジョン放送信号等を録画することが多く行われており、CATV等の有料放送であっても自由に録画している状態になっている。かかるCATVの有料放送では信号が暗号化されて放送され、特定のデコーダを有する者のみが復号して視聴することができる。

有料放送のテレビジョン信号を記録する場合には、暗号化(スクランブル)されて送られたテレビジョン信号をそのまま記録するか、一旦復号化(デスクランブル)して通常の映像信号にしてから記録するかのいずれかであった。

発明が解決しようとする課題

ところが、このような暗号化されている有料放送の信号をデスクランブルして記録する場合には、もはや通常の映像信号になってしまっているために自由にテープを再生できることとなり、不正複

写を防げないために有料放送の意味がなくなってしまふ。

一方、スクランブル化されているままで記録する場合には、その解読用の鍵(キー)が時間の経過で(たとえば年、月、週、日等の単位で)変更されると解読できなくなる。解読鍵(キー)が変更されなければ、その解読鍵(キー)を保持している有料デコーダであればどの有料デコーダを用いてもテープを再生してデスクランブルして視聴することができることになる。従って、この場合にもスクランブル化されたままのテレビジョン信号を記録したテープを不正複写して盗視聴することができ、有料放送の意味がなくなることになる。

そこで、本発明は、かかる従来の問題点を解消して、不正複写しても盗視聴することができないような信号記録装置を提供することを目的とするものである。

課題を解決するための手段

かかる目的を達成するために、本発明においては、少なくともテレビジョン信号の映像信号と音

声信号を記録再生する装置において、スクランブル化されたテレビジョン信号を復号するデコーダからそのデコーダに固有の鍵 $K_i$ を用いて暗号化された解読鍵 $K_t$ を読み出すための駆動信号を出力する手段と、この暗号化された解読鍵 $K_t$ をテレビジョン信号中の水平または垂直の帰線期間またはその近傍で記録可能な部分に多重化する手段と、再生信号から暗号化された解読鍵 $K_t$ を抽出し制御信号と共にデコーダへ再生信号を供給する手段とを備えたことを特徴とする。

作用

かかる構成により、各デコーダで固有の鍵 $K_i$ を用いて解読鍵 $K_t$ を暗号化したものを記録するようにしているため、その鍵 $K_i$ を有するデコーダ以外のデコーダでは再生することができようにすることができ、しかも、このような記録をデコーダと独立して記録装置側で記録信号に多重化して行うことができる。

実施例

本発明の一実施例を第1図に示す。図中、1～

9の部分は記録再生装置(たとえばVTR)であり、11～16の部分は暗号解読機能及び暗号化機能を含む有料デコーダの一部を示す。

第1図中、同期分離回路1、記録ヘッド6、再生ヘッド8及び図示していない他の部分は通常のVTRの該当部分と共通の回路等である。また、有料デコーダの図示していない部分たとえばデータ抜取回路、暗号復号回路等は既に実用化されている有料放送(例えばVideo Cipher IIやBMAC等)の有料デコーダの当該部分と機能的に同一の回路である。

まず、本発明のシステムの基礎となる暗号化システム全体の概要を第2図、第3図を参照して説明する。ここでは、時間の経過により変化する鍵 $K_t$ によって一義的に決まる関数 $f(K_t)$ により映像信号及び音声信号をスクランブル化するものとする。鍵 $K_t$ を送出側から受信側へ伝送する場合、そのままの形では盗聴されるおそれがあるので、別の鍵 $K_i$ で暗号化する。鍵 $K_i$ は、端末1台ずつに別々のものを割当てる。このような鍵の

重層構造については、たとえば、一松信監修「データ保護と暗号化の研究」第3頁図1-27等に記載されている。鍵 $K_t$ と $K_i$ の間に、もう一つ鍵 $K_x$ より長い周期で更新される鍵 $K_x$ を用いてもよい。このことも同文献に示されている。第3図がその例である。

ここでは、説明を簡単にするために、第2図の場合について説明する。放送の形式として、鍵等の制御信号をデジタル信号で送出できる放送衛星BS2で採用されている方式を考える。この方式は、音声をデジタル信号で伝送するので、その音声データにPN信号を加算すれば暗号化(スクランブル化)できる。従って、そのPN信号の初期値がすなわち鍵 $K_t$ となり、これが判れば復号化(デスクランブル化)できる。この鍵 $K_t$ を鍵 $K_i$ で暗号化(スクランブル化)して送り、受信側で鍵 $K_i$ で復号化すればよい。映像信号については、ラインローテーションによる暗号化(スクランブル化)を行ない、その各ラインでの切断点を上記PN信号で与えればよく、これについては

公知の技術が使える。

さて、第1図において、有料デコーダでは受信信号（例えばB SチューナーのFM検波複合映像出力信号）がそのまま入力される。その信号から、5.73 MHzの音声搬送波成分と映像信号成分とを分離し、5.73 MHzのQPSK信号を復調して2.048 Mbpsのデジタル信号を得る。QPSK復調回路の出力から音声データ以外の制御信号データを抜き取り、その制御信号データから暗号化されている鍵 $K_t$ その他の信号を復号し、復号化出力中の鍵 $K_t$ を $K_t$ メモリA11に記憶する。なお、メモリA11の他に鍵 $K_t$ 以外の制御信号を記憶するメモリが別にあることはいうまでもない。

以下の説明では $K_t$ は毎週変化するものとし、端末側では、毎週1回固有の鍵 $K_i$ で、第4図Bの信号を解読するものとする。鍵 $K_t$ の配送は例えば月～金の間毎日行ない、第1図の $K_t$ メモリA11内を2個の $K_t$ 分の容量とし、毎週日曜日の午前零時に切替える等の操作で端末内の鍵 $K_t$ は、その週の鍵 $K_t$ に切替わる。さて、 $K_t$ メモ

リ11内にその週の鍵 $K_t$ （以下 $K_{t1}$ と記す）がメモリされているものとする。一方、第1図一点鎖線の右側はVTRである。P1にスクランブルされた映像信号が入力される。なお、音声については簡単の為、デスクランブル化され、左と右のベースバンド音声信号で記録されるものとする。

この映像信号は、垂直及び水平の同期信号の部分はスクランブル化されず、他の部分はいわゆる公知のラインローテーションによりスクランブル化されているものとする。

端子P1への入力を同期分離回路1で分離し、HパルスとVパルスを得る。第5図に示す如く、R/W制御回路2へ、記録指示回路9から時刻 $t_1$ で、記録指示パルスが供給されると、その後の垂直帰線期間の始めの部分で、R/W制御回路2からデコーダの読出制御回路13へ $t_1'$ から始まる読出クロック $\phi_3$ が供給される。一方、読出制御回路13へは、 $t_1$ から制御パルス $\phi_2$ が供給され、 $K_t$ メモリA11の内容 $K_t$ を暗号器12で固有の鍵 $K_i$ を用いて暗号化して暗号化鍵信号 $KK_i$

( $K_t$ )を作る。 $t_1'$ から暗号器12内の $KK_i$ ( $K_t$ )を読み出しバッファメモリ3へ記憶する。バッファメモリ3の内容を $t_2 \sim t_3$ 間にクロック $\phi_4$ で読み出し、第6図に示す如くテレビジョン信号の第22H目に重畳する。混合回路4では、ラインローテーションによりスクランブル化された第22H目の映像信号を除去し、第4図のBの $KK_i$ ( $K_t$ )信号を重畳する。これを記録ヘッド6によりテープに記録する。テープの高域特性が悪ければ、288ビットを2Hに分けて記録しても支障はない。

他のスクランブル内容に関する信号は、垂直帰線期間(VBI)の例えば第20H目（又は第20H目と第21H目の合計で288ビット）に288ビット、第6図の如く重畳されているものとする。この結果、VTRのテープには、 $\phi_5$ の如く $t_2 \sim t_3$ に第4図Bの信号を含んだ形で、即ち $\phi_6$ に $t_2 \sim t_3$ の部分を追加した形で記録される。

次に、記録信号 $\phi_5$ を再生する場合を説明する。

読出ヘッド部6でテープから記録信号 $\phi_5$ を読み出し、信号分離回路7へ伝える。信号分離回路7で第6図の信号中のヘッダ（第4図のA、Bのヘッダ部）を検出し、制御信号形成回路8で制御信号 $\phi_6$ を形成し、この $\phi_6$ を有料デコーダの入出力制御部16へ供給する。制御部16から $K_i$ ( $K_t$ )デコーダ14と、入力バッファメモリ15へクロックを送る。即ち、入力バッファメモリ15のメモリへ第6図の $t_2 \sim t_3$ からの288ビット（第4図Aに相当）を書込み、続いて、デコーダ14へ入力バッファメモリ15の内容を転送し、その有料デコーダに固有の鍵 $K_i$ で解読して、鍵 $K_t$ を取り出し、 $K_t$ メモリB17へ書き込む。

VTR出力を有料デコーダに入力する場合、有料デコーダに切替スイッチを設けておき、そのスイッチの切替えにより $K_t$ メモリA11の中の鍵 $K_t$ を使うか $K_t$ メモリB17の中の鍵 $K_t$ を使うかを切替える。従って、VTRの再生出力をデスクランブル化する場合は、 $K_t$ メモリB17の中鍵 $K_t$ 即ち、VTRテープに記録されている信号

をスクランブル化するために用いた暗号鍵  $K_t$  を用いるので、デスクランブル化できる。これは、記録する時に用いた有料デコーダによってのみ可能となる。

なお、送られてくる鍵  $K_t$  が変更される迄の間は、他の有料デコーダで記録したスクランブル済の信号を別の有料デコーダで再生することは、有料デコーダの内部結線を変更すれば可能であるが、有料デコーダ側で  $K_t$  メモリ A 11,  $K_t$  メモリ B 17、その切替部分をパッケージ化してモールドする等の方法でその結線変更を不可能にすれば防止できる。

以上の説明は、鍵の重層構造が第2図の如く2層の場合であるが、第3図の如く3層であってもよい。3層の場合、鍵  $K_t$  でなく鍵  $K_x$  を鍵  $K_i$  で暗号化して記録し、再生し、第1図の  $K_t$  メモリ A 11 と  $K_t$  メモリ B 17 には鍵  $K_x$  を記憶させる。

#### 発明の効果

このように、本発明によれば、時間と共に変更

される鍵の更新周期を短かくしておけば、一つの有料デコーダを用いて記録したスクランブル化された信号は他の有料デコーダではデスクランブル化できないので、不法な複写を防止できる。

また、有料デコーダの内部構造で物理的に保護すれば、鍵が変化する前でも、他の有料デコーダを用いて記録したスクランブル化された信号をデスクランブル化することはできない。なぜならば、再生して得られる信号から鍵  $K_i$  を用いて解読しても鍵  $K_t$  が得られず、一方、有料デコーダで構造的に再生時は再生出力から得られた鍵のみを使えるように構成しておき、その構造を外部より変更できないようにしておくことができるからである。

#### 4、図面の簡単な説明

第1図は本発明の一実施例における信号記録装置のブロック図、第2図、第3図はその暗号化、復号化の原理を示すブロック図、第4図、第5図、第6図はその動作を示す波形図である。

1 ……同期分離回路、2 ……R/W制御回路、

3 ……バッファメモリ、4 ……混合回路、5 ……記録ヘッド部、6 ……読出ヘッド部、7 ……信号分離回路、8 ……制御信号形成回路、9 ……記録指示回路、11 …… $K_t$  メモリ A、12 ……暗号器、13 ……読出制御回路、14 ……デコード回路、15 ……入力バッファメモリ、16 ……入出力制御回路、17 …… $K_t$  メモリ B。

代理人の氏名 弁理士 栗野重孝 ほか1名

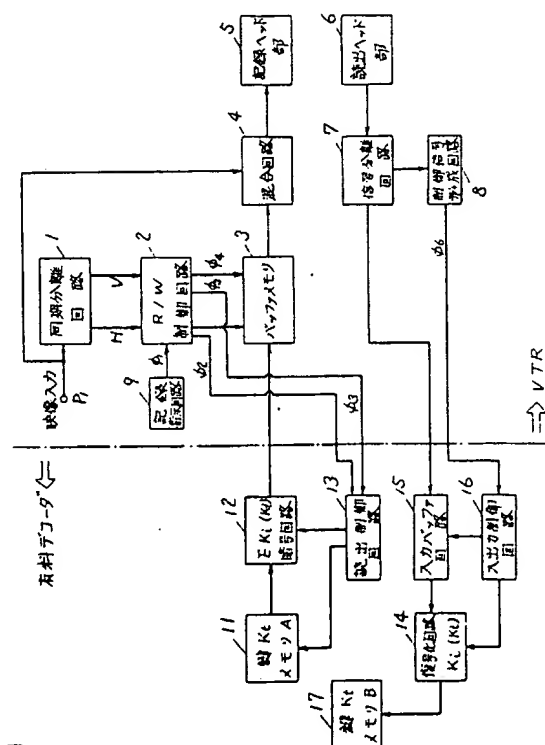
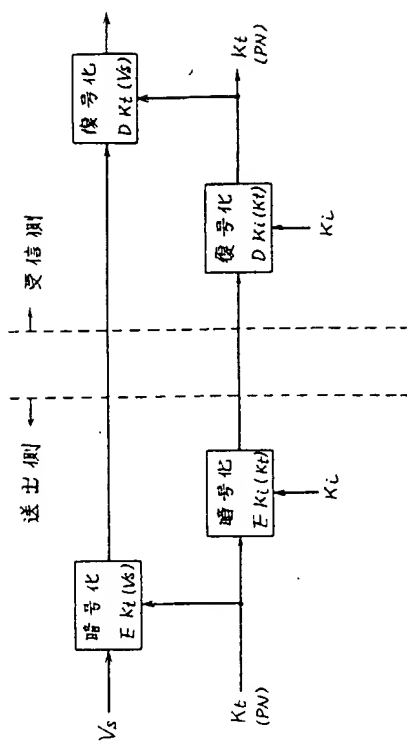
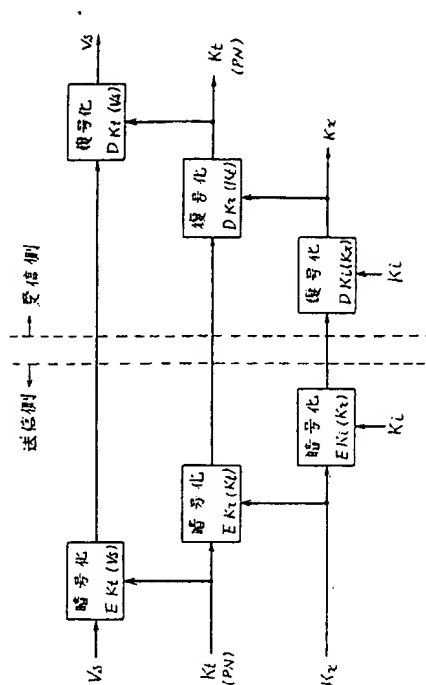


図 1

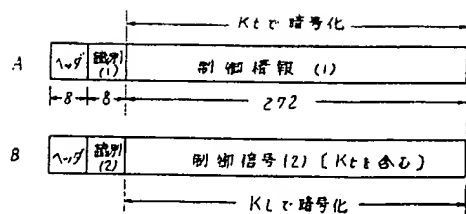
第 2 図



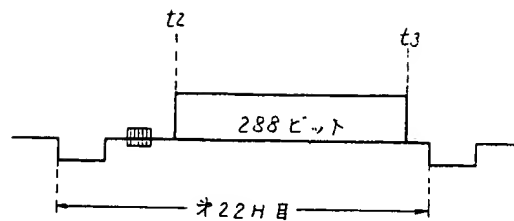
第 3 図



第 4 図



第 6 図



第 5 図

